

ABSTRACT

A system and method that facilitate secure communication employing dialog session keys that can be shifted unilaterally is provided. A key exchange key can further be employed to encrypt and/or decrypt the dialog session keys that are used to encrypt and/or decrypt message(s) that form a dialog between services. For example, the key exchange key can be unique to a service pair, while a first dialog session key is unique to message(s) originated by a first service, and, a second dialog session key is unique to message(s) originated by a second service.

The system allows the dialog session keys to be independently managed by each endpoint (*e.g.*, service). This makes updating the dialog session key very easy and lightweight compared to other messaging systems, where both endpoints must agree on the updated session key. An endpoint can shift the dialog session key for message(s) it originates based on a dialog session key policy (*e.g.*, time-based, upon receipt of a change in the second dialog session key, and/or receipt of shifts of shifts the second dialog session key more than a threshold quantity of times in a given time period).